UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/664,069	09/16/2003	Cheh Goh	300110535-2	3247

22879 7590 04/01/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
04/01/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/664,069
Filing Date: September 16, 2003
Appellant(s): GOH ET AL.

David Millers
Reg. No. 37396
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on 11/16/2009 appealing from the Office action mailed on 16/16/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) **Evidence Relied Upon**

Peinado, US 2002/0013772 A1 01-2002.

Lampson et al. US 2003/0196099 A1 10-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 1-4, 11-18, 25-28, 30, 31 and 35-38 rejected under 35 U.S.C. 103(a) as being unpatentable over Peinado US 2002/0013772 A1 in view of Lampson et al. US 2003/0196099 A1 (hereinafter Lampson).

As per claims 1 and 11-13, Peinado teaches a system comprising:

an output device for outputting data onto a removable storage medium (i.e., figure 13, portable device) ;

a first computing entity arranged to encrypt a first data set (i.e., content), the encrypting done by the first computing entity being based on encryption parameters comprising public data of a trusted party (i.e., PU-BB-PD) and an encryption key string (i.e., content key, KD) comprising a second data set that defines a policy for allowing the output of the first data set onto a said removable storage medium (i.e., license/sub-license), the first computing entity being further arranged to output the encrypted first data set for the output device (i.e., content being encrypted according to content key, content key being encrypted according to PU-BB-PD/black box public key, and delivering the encrypted content and sub-license to the portable device, see paragraphs 0278, 0284-0292); and

a second computing entity associated with the trusted party and arranged when satisfied that said policy has been met, to output for the output device a decryption key, for use in decrypting the encrypted first data set, the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data (i.e., the portable device/black box decrypting the content key by using private key, PR-BB-PD, that is related to the public key, see paragraphs 0278, 0284-0292);

the output device being arranged to use the decryption key in decrypting the encrypted first data set (i.e., the portable device using the content key and decrypting the content, see paragraphs 0278, 0284-0292). Peinado is silent on the encryption key being distinct from the decryption key. However, it is well known to have an encryption key that is distinct from a decryption key for enhancing security of the system. For example, Lampson teaches an encryption/decryption system, including an encryption key that is distinct from a decryption key [see at least the abstract]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Lampson within the system of Peinado in order to enhance the security of the system.

As per claims 15, 25 and 26, Peinado teaches a data output method comprising the steps of:

(a) encrypting a first data set the encrypting done by the first computing entity being based on encryption parameters comprising public data of a trusted party (i.e., PU-BB-PD) and an encryption key string (i.e., content key) comprising a second data set that defines a policy (i.e., license/sub-license) for allowing the output of the first data set to a removable storage medium (i.e., content being encrypted according to content key, content key being encrypted according to PU-BB-PD/black box public key, and delivering the encrypted content and sub-license to the portable device, see paragraphs 0278, 0284-0292),

(b) providing the encrypted first data set to an output device adapted to output data to a removable storage medium (i.e., delivering the encrypted content and sub-license to the portable device, see paragraphs 0278, 0284-0292);

(c) at the trusted party (portable device black box) checking that said policy has been satisfied and thereafter providing the output device with a decryption key, for use in decrypting

the encrypted first data set, this decryption key being generated in dependence on the encryption key string and private data related to said public data (i.e., the portable device/black box decrypting the content key by using private key, PR-BB-PD, that is related to the public key, see paragraphs 0278, 0284-0292); and

(d) at the output device using the decryption key in decrypting the encrypted first data set and outputting the first data set to a removable recording medium (i.e., the portable device using the content key and decrypting the content, see paragraphs 0278, 0284-0292).

Peinado is silent on the encryption key being distinct from the decryption key. However, it is well known to have an encryption key that is distinct from a decryption key for enhancing security of the system. For example, Lampson teaches an encryption/decryption system, including an encryption key that is distinct from a decryption key [see at least the abstract]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Lampson within the system of Peinado in order to enhance the security of the system.

As per claims 28, 30, 31 and 35-37, Peinado teaches a printing system comprising:

a printer [paragraphs 036, 0099, 0267];

a first computing entity arranged to encrypt a first data set (i.e., content) the encrypting done by the first computing entity being based on encryption parameters comprising public data of a trusted party (i.e., PU-BB-PD) and an encryption key string (i.e., content key, KD) comprising a second data set that defines a policy for allowing the output/printing of the first data set onto a said removable storage medium (i.e., license/sub-license), the first computing entity being further arranged to output the encrypted first data set for the output device/printing device (i.e., content being encrypted according to content key, content key being encrypted

according to PU-BB-PD/black box public key, and delivering the encrypted content and sub-license to the portable device, see paragraphs 0278, 0284-0292); and

a second computing entity associated with the trusted party and arranged when satisfied that said policy has been met, to output for the output device a decryption key, for use in decrypting the encrypted first data set, the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data (i.e., the portable device/black box decrypting the content key by using private key, PR-BB-PD, that is related to the public key, see paragraphs, 0278, 0284-0292);

the output device/printer being arranged to use the decryption key in decrypting the encrypted first data set (i.e., the portable device using the content key and decrypting the content, see paragraphs 0278, 0284-0292).

Peinado is silent on the encryption key being distinct from the decryption key. However, it is well known to have an encryption key that is distinct from a decryption key for enhancing security of the system. For example, Lampson teaches an encryption/decryption system, including an encryption key that is distinct from a decryption key [see at least the abstract]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Lampson within the system of Peinado in order to enhance the security of the system.

As per claims 2 and 16, Peinado further teaches the system wherein the second computing entity is arranged to generate the decryption key only when said policy has been met [see paragraphs, 0278, 0284-0292].

As per claims 3 and 17, Peinado further teaches the system wherein the second computing entity is arranged to issue to the first computing entity at least one of: the second data set, the encryption key string, a derivative of the encryption key string usable by the first computing entity, in place of the encryption key string, in the encryption of said first data set [paragraphs 0278, 0284-0292].

As per claims 4 and 18, Peinado further teaches the system wherein the second computing entity is arranged to receive the encryption key string directly or indirectly from the first computing entity [paragraphs 0278, 0284-0292].

As per claims 14, 27 and 38, Peinado further teaches the system further comprising a portable device comprising the second computing entity and a first communications interface, the output device comprising a second communications interface arranged to cooperate with the first communications interface to enable communication between the second computing entity and the output device, the communications interfaces being such that the portable device must be present at the output device for the communication between the second computing entity to take place [see figure 13].

Allowable Subject Matter

Claims 5-10, 19-24, 29 and 32-34 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

(10) Response to Argument

With respect to independent claim 1:

Appellant argues that, the combination of Peinado and Lampson fails to teach 'a first computing entity for encrypting a first data set, the first computing entity encrypting the first data set based on encryption parameters that comprise: public data of a trusted party, and an encryption key string comprising a second data set that defines a policy for allowing the output of the first data set onto said removable storage medium.' The combination of Peinado and Lampson fails to suggest encryption based on an encryption key string that defines a policy for allowing output.

Examiner would point out that, Peinado teaches a first computing entity arranged to encrypt a first data set (i.e., content), the encrypting done by the first computing entity being based on encryption parameters comprising public data of a trusted party (i.e., PU-BB-PD) and an encryption key string (i.e., content key, KD) comprising a second data set that defines a policy for allowing the output of the first data set onto a said removable storage medium (i.e., In composing the sub-license the content key is re-encrypted for decrypting content, paragraphs 0284-0285)

Appellant argues that, Peinado and Lampson fail to teach or suggest encryption 'based on encryption parameters that comprise: ... an encryption key string ... that defines a policy for allowing the output.' Appellant further argues that, Peinado and Lampson fail to lead one of ordinary skill in the art to leap to the idea of using an output policy as an encryption key string

Examiner would point out that, Peinado teaches a first computing entity arranged to encrypt a first data set (i.e., content), the encrypting done by the first computing entity being based on encryption parameters comprising public data of a trusted party (i.e., PU-BB-PD) and

an encryption key string (i.e., content key, KD) comprising a second data set that defines a policy for allowing the output of the first data set onto a said removable storage medium (i.e., license/sub-license' Note that, the content key is re-encrypted and tied to the license (policy), see paragraphs 0278, 0284-0292). Furthermore, Peinado is silent on the encryption key being distinct from the decryption key. However Lampson teaches an encryption/decryption system, including an encryption key that is distinct from a decryption key [see at least the abstract]. One of ordinary skill in the art would have been motivated to do so because having a different encryption key from the encryption key as taught by Lampson would enhance security of the system because such a system would prevent attacker that have knowledge of the encryption key from decrypting an encrypted content.

With respect to claims 2-4, 11-18, 25-28, 30, 31 and 35-48 appellant argues that, the claims are patentable over Peinado and Lampson for at least the same reasons that claims 1 is patentable over Peinado and Lampson.

Examiner would point out that arguments with respect to claim 1 have been traversed as indicated above and therefore, arguments with respect to claims 2-4, 11-18, 25-28, 30, 31 and 35-48 have been traversed with the same reason applied thereto.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Beemnet W Dada/
Primary Examiner, Art Unit 2435

Conferees:

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435

/Hosuk Song/

Primary Examiner, Art Unit 2435